REMARKS

Applicants respectfully request reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. Claims 1, 8, 19, 20, and 24 have been amended.

After amending the claims as set forth above, Claims 1-25 are pending in the application.

I. Amendments to the Claims

As indicated above, Claims 1, 8, 19, 20, and 24 have been amended to clarify the claimed subject matter and to correct possible antecedent basis issues and typographical errors. Applicants respectfully submit that no new matter has been added to the application.

These amendments place the claims either in condition for allowance or in better condition for appeal. The amendments do not necessitate a new search. As such, the amendments and remarks should be entered.

II. Claim Rejections Under 35 U.S.C. § 102

On page 2 of the Office Action, Claims 1-25 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,050,396 to Cohen *et al.* (hereinafter "Cohen"). Applicants respectfully traverse the rejection. Claims 1, 8, 19, 20, and 24 have been amended to clarify the claimed subject matter and correct typographical errors.

A. Claims 1, 8, 15, 17, 19, and 24

As amended, independent Claim 1 is:

> A system for managing quality of service (QoS) for traffic flows generated by a plurality of hosts separated by one or more networks wherein at least one of the networks is enabled with a set of traffic classes, said system comprising:
>
> a services manager, and

a middleware module at at least one of the plurality of hosts, wherein said middleware module at the one host receives a QoS request for a traffic flow the host generates and conveys a QoS provisioning request to the services manager upon receiving the QoS request for the traffic flow, and

wherein said services manager receives the QoS provisioning request from said middleware module, obtains a DSCP (Differentiated Services Code Point) value for the traffic flow only if it is determined that the networks the traffic flow traverses can support the flow, and if a DSCP value is obtained, conveys the obtained DSCP value for the traffic flow to said middleware module, and

wherein said middleware module uses the obtained DSCP value received from the services manager to mark the DSCP field of packets of the traffic flow.

(Emphasis added). As amended, independent Claim 8 recites, in part:

A services manager ... comprising:

means for receiving a QoS provisioning request from a middleware module for any given traffic flow, ...

means for obtaining a DSCP (Differentiated Services Code Point) value for the given traffic flow based on whether the networks the traffic flow traverses can support the flow given the determined traffic attributes, ...

(Emphasis added). Independent Claim 15 recites, in part:

A system ... comprising:

a middleware control module for receiving QoS provisioning requests for the plurality of traffic flows and for conveying the requests to a services manager ... .

(Emphasis added). As amended, independent Claim 17 recites, in part:

A system ... comprising:

a signaling client for generating QoS provisioning requests for one or more of the plurality of traffic flows,

> a middleware control module for receiving the QoS provisioning requests and for conveying the requests to a services manager … .

(Emphasis added). As amended, independent Claim 19 recites, in part:

> A method … comprising:
>
> receiving, at a services manager, a QoS provisioning request from a middleware module for any given traffic flow, …
>
> obtaining a DSCP (Differentiated Services Code Point) value for the given traffic flow based on whether the networks the traffic flow traverses can support the flow given the determined traffic attributes … .

(Emphasis added). As amended, independent Claim 24 recites, in part:

> A method … comprising:
>
> receiving, at a middleware module, a QoS provisioning request for any given traffic flow,
>
> conveying the request from the middleware module to a services manager … .

i. Cohen fails to disclose receiving a QoS request at a middleware module.

Claim 1 recites, in part, a "middleware module at the one host receives a QoS request for a traffic flow the host generates." Claims 15, 17, and 24, though different in scope, recite similar elements. Applicants respectfully submit that Cohen fails to teach, suggest, or disclose such an element.

On page 2 of the Office Action, the Examiner asserts that Cohen discloses:

> a middleware module at at least one of the plurality of hosts, wherein said middleware module at the one host receives a QoS request for a traffic flow the host generates and conveys the QoS provisioning request to the services manager upon receiving the QoS request for the traffic flow (column 6, lines 35-45, column 8, lines 19-25).

Applicants respectfully disagree. Column 6, lines 35-45 of Cohen states:

> Network devices 220, 222 represent edge network devices such as routers, switches, or other similar or equivalent devices that are configured for coloring packets within network 228. In one embodiment, network devices 220, 222 are configured to execute the Cisco Internetworking Operating System (IOS) and are capable of marking packets with DSCP values, i.e., they are compatible with Differentiated Services. Such marking may be carried out using a marker or other software element or application that runs under control of IOS, e.g., an agent or process.

(Emphasis added). Column 8, lines 7-11 and 19-25 of Cohen states:

> [A] quality of service policy is created and stored in association with an edge device such that a specified DSCP reflective signaling value in packets of inbound flows is detected, and the same DSCP value is applied to corresponding return flows.
>
> A reflective DSCP feature may be configured on edge devices 220, 222 in several ways. In one approach, the incoming DSCP value is specified along with the DSCP value that should be sent reflected. This can be augmented by specifying that reflection should be done only for packets coming from a specific subnet, or any other additional restrictions of the set of flows being reflected.

(Emphasis added). Applicants respectfully submit that these portions of Cohen cited by the Examiner, along with the rest of Cohen, fail to teach, suggest, or disclose a "middleware module ... receives a QoS request for a traffic flow ... and conveys a QoS provisioning request to the services manager upon receiving the QoS request" as in amended Claim 1.

The above quoted portions of Cohen appear to disclose edge network devices "that are capable of marking packets with DSCP values." In addition, Cohen appears to disclose that a **QoS policy** is created and stored that corresponds to an edge device and that this **QoS policy specifies** that DSCP value should be sent in a reflected flow based on an incoming DSCP value. However, these portions of Cohen fail to disclose any type of **request**. Accordingly, Cohen fails to teach, suggest, or disclose a "QoS request for a traffic flow" being received at a middleware

module or "conveying a QoS provisioning request to a services manager upon receiving the QoS request." If the Examiner believes such a request is disclosed by Cohen, Applicants respectfully request that the Examiner specifically point out where in Cohen a "QoS request" is received by a "middleware module."

ii. Cohen fails to disclose sending the request from the middleware module to a service manager.

Claim 1 recites, in part, a "middleware module ... conveys a QoS provisioning request to the services manager" and "wherein said services manager receives the QoS provisioning request from said middleware module." Claims 8, 15, 17, 19, and 24, though different in scope, recite similar elements. Applicants respectfully submit that Cohen fails to teach, suggest, or disclose these elements.

On page 3 of the Office Action, the Examiner asserts that Cohen discloses:

> wherein said services manager receives the QoS provisioning request from said middleware module, obtains a DSCP (Differentiated Services Code Point) value for the traffic flow if the networks the traffic flow traverses can support the flow, and if a DSCP value is obtained, conveys the obtained DSCP value for the traffic flow to said middleware module (column 7, lines 13-20, 33-40, column 8, lines 8-16).

Applicants respectfully disagree. Column 7, lines 13-20 and 33-40 of Cohen states:

> Policy Management Station 202 is a computer, or a group of hardware or software components or processes that cooperate or execute in one or more computer systems. In this example, Policy Management Station 202 includes one or more policy servers 206, 208, 210, that are coupled to network devices 220, 222, 224, 226. In one embodiment, a policy coordinator communicates with policy servers 206, 208, 210 to configure the network devices 220, 222, 224, 226, to control the coloring and forwarding of packets within network 228. ...
>
> In one embodiment, Policy Management Station 202 provides a

> mechanism whereby a network administrator may select or define a desired service level that is to be applied to a particular group of data flows within network 206. For example, an administrator may choose to have a service level of Gold be applied to all VOIP flows within computer network 200. In response, the policy coordinator communicates with the policy servers to cause edge devices 220, 222 to set an initial DSCP value in the packets of all VOIP flows.

(Emphasis added). Applicants respectfully submit that these portions of Cohen cited by the Examiner along with the rest of Cohen fails to teach, suggest, or disclose a "middleware module ... conveys a QoS provisioning request to the services manager upon receiving the QoS request" or a "services manager receiving a QoS provisioning request from a middleware module" as in amended Claim 1.

The above quoted portions of Cohen disclose a "policy coordinator" that communicates with "policy servers" to "configure the network devices", however a "QoS provisioning request" is not disclosed as being communicated between any of the elements. Cohen also appears to disclose that a person such as a network administrator may define a service level of a group of data flows. However, Cohen fails to disclose receiving a "QoS provisioning request" at a "services manager" from a "middleware module." If the Examiner still believes such a request is disclosed by Cohen, Applicants respectfully request that the Examiner specifically point out where Cohen discloses a "QoS provisioning request" is received by a "services manager" from a "middleware module."

iii. Cohen fails to disclose obtaining a DSCP value "if the networks the traffic flow traverses can support the flow."

As amended, Claim 1 recites, in part, "obtain[ing] a DSCP ... value for the traffic flow only if it is determined that the networks the traffic flow traverses can support the flow." Claims 8 and 19, though different in scope, recite similar elements. Applicants respectfully submit that Cohen fails to teach, suggest, or disclose such an element.

On page 3 of the Office Action, the Examiner asserts that Cohen discloses "wherein said services manager ... obtains a DSCP (Differentiated Services Code Point) value for the traffic flow only if the networks the traffic flow traverses can support the flow... (column 7, lines 13-20, 33-40, column 8, lines 8-16)." On page 10 of the Office Action, the Examiner further asserts:

> A network may be configured to run hop behaviors such as Best Effort, Expedited Forwarding, and Less than Best Effort. A QoS policy is selected that colors packets with the DSCP value for the Best Effort, Expediting Forwarding, and Less than Best Effort. According to what the network can perform, a DSCP value is given to the packet to execute the policy for the flow (column 3, lines 41-50, column 4, lines 1-21, column 6, lines 35-55, column 7, lines 22-32).

(Emphasis added).

Applicants respectfully disagree. Applicants respectfully assert that these portions, and the rest of Cohen, fail to teach, suggest, or disclose obtaining a DSCP value "only if the networks the traffic flow traverses can support the flow" as in amended Claim 1.

Column 3, lines 41-50; column 4, lines 1-21; column 6, lines 35-55; and column 7, lines 22-32 of Cohen state:

> Currently, a Differentiated Services (DS) architecture is under development by the Internet Differentiated Services Working Group of the Internet Engineering Task Force (IETF). The main idea behind DS is the classification and possibly conditioning of traffic at network boundaries. The classification operation entails the assignment of network traffic to behavioral aggregates. The behavioral aggregates define a collection of packets with common characteristics that determine how they are identified and treated by the network. ...
>
> In a typical differentiated services environment, DS nodes located at the border of the DS domain ("edge devices") mark or "color" each IP packet for a particular flow with a specific DSCP value based on the currently established QoS policies. Such coloring may involve loading the DS field 132 of a packet with a particular

DSCP value. Thereafter, the interior DS compliant devices along the path apply the corresponding forwarding behavior to the packet based on the particular DSCP value.

For example, a QoS policy typically includes a filter or Boolean expression that indicates which packets are to be colored, and with what DSCP values. For example, **a network administrator may configure its network to run three per hop behaviors end to end, such as Best Effort (BE), Expedited forwarding (EF) and a PHB behavior for background traffic that can be named "less than best effort" (LBE).** The network administrator can now select a QoS policy that colors all Voice Over IP (VOIP) packets with the standard DSCP value for the EF PHB and marks all email packets with the DSCP value used to indicate a LBE per hop forwarding behavior. ...

Network devices 220, 222 represent edge network devices such as routers, switches, or other similar or equivalent devices that are configured for coloring packets within network 228. In one embodiment, network devices 220, 222 are configured to execute the Cisco Internetworking Operating System (IOS) and are capable of marking packets with DSCP values, i.e., they are compatible with Differentiated Services. Such marking may be carried out using a marker or other software element or application that runs under control of IOS, e.g., an agent or process. Network devices 224, 226 represent internal network devices such as routers, switches, or other similar or equivalent devices that are configured for forwarding packets within network 228 based [on] the color of each packet. In certain embodiments, network devices 224, 226 are configured to execute the Cisco Internetworking Operating System (IOS) and are capable of forwarding packets based on their DSCP values, i.e., they are compatible with Differentiated Services. It should be noted that network devices 220, 222 and network devices 224, 226 may in fact represent similar or even identical device types and/or models that are each configured to perform a designated function within computer network 200. ...

For example, the policy coordinator may direct network devices 220, 222 to color the packets of all Voice Over IP (VOIP) flows with the color gold (high priority) and to color the packets of all File Transfer Protocol (FTP) flows with the color Bronze (low priority). Each color corresponds to a particular service level and is

> associated with one or more QOS treatment parameters, e.g., a pre-defined DSCP value and possibly other values or characteristics. The policy coordinator may further direct network devices 224, 226 to apply a particular forwarding policy based on the particular color of each packet that is processed.

As such, Cohen appears to teach that a network administrator may configure a network to run "three hop behaviors" such as "Best Effort, Expedited Forwarding, and Less than Best Effort." However, Cohen fails to disclose what such a configuration entails. Cohen also teaches that a network administrator can select a QoS policy that colors certain packets according to the "three hop behavior." DS nodes may then color the packets according to the policy. However, no determination is made about whether the network (that the traffic flow traverses) can support the flow. Accordingly, Cohen fails to disclose "obtain[ing] a DSCP ... value for the traffic flow only if it is determined that the networks the traffic flow traverses can support the flow" as in amended Claim 1. If the Examiner still believes that such an element is shown by Cohen, Applicant respectfully requests that the Examiner specifically point out where in Cohen "it is determined that the networks the traffic flow traverses can support the flow."

For at least the reasons discussed above, Applicants respectfully submit that Claims 1, 8, 15, 17, 19, and 24 are in condition for allowance. As such, Applicants request reconsideration and withdrawal of the rejection of Claim 1, 8, 15, 17, 19, and 24 and the various claims which depend therefrom.

B. Claim 2

Claim 2 recites, in part, "wherein the services manager ... as part of obtaining the DSCP value further determines if for each traffic class enabled network the traffic flow traverses there is sufficient bandwidth in a traffic class to support the traffic flow." (Emphasis added). Claims 11 and 12, though different in scope, recite similar elements. Applicants respectfully submit that Cohen fails to teach, suggest, or disclose such an element.

On page 3 of the Office Action, the Examiner asserts that Claim 2 is disclosed by "column 7, lines 35-50" of Cohen. Column 7, lines 35-50 of Cohen states:

> For example, an administrator may choose to have a service level of Gold be applied to all VOIP flows within computer network 200. In response, the policy coordinator communicates with the policy servers to cause edge devices 220, 222 to set an initial DSCP value in the packets of all VOIP flows. An example of a commercial product suitable for use as Policy Management Station 208 is CiscoAssure QoS Policy Manager 1.0, commercially available from Cisco Systems, Inc.
>
> Although the example embodiment of FIG. 2 shows two (2) workstations 216, 218, three (3) policy servers 216, 208, 210, two (2) edge devices 220, 222, and two (2) internal devices 224, 226, in other practical embodiments there may be any number of such elements.

(Emphasis added). Column 7, lines 35-50 of Cohen discloses that an administrator may select a service level for a specific flow and that a "policy coordinator" and "policy servers" cause edge devices to set DSCP values in the packets of the specific flow. However, Cohen fails to disclose any type of determination of the capabilities of the network which the flow traverses. Cohen further fails to disclose any type of determination of a bandwidth capacity of the network. As such, Applicants respectfully submit that Cohen fails to teach, suggest, or disclose "wherein the services manager ... as part of obtaining the DSCP value further determines if for each traffic class enabled network the traffic flow traverses there is sufficient bandwidth in a traffic class to support the traffic flow" as in Claim 2.

For at least the reasons discussed above, Applicants respectfully submit that Claims 2, 11, and 12 are in condition for allowance. As such, Applicants request reconsideration and withdrawal of the rejection of Claims 2, 11, and 12.

C. Claim 4

Claim 4 recites, in part, "wherein if the services manager cannot obtain a DSCP value ... , the services manager determines an alternate traffic flow characterization for the traffic flow based on the traffic flow identification." (Emphasis added). Claims 14 and 23, though different in scope, recite similar elements. Applicants respectfully submit that Cohen fails to teach, suggest, or disclose such an element.

On page 4 of the Office Action, the Examiner asserts that Claim 4 is disclosed by "column 7, lines 25-37 [and] column 10, lines 33-49" of Cohen. Applicants respectfully disagree. Column 7, lines 25-37 of Cohen states:

> Each color corresponds to a particular service level and is associated with one or more QOS treatment parameters, e.g., a pre-defined DSCP value and possibly other values or characteristics. The policy coordinator may further direct network devices 224, 226 to apply a particular forwarding policy based on the particular color of each packet that is processed.
>
> In one embodiment, Policy Management Station 202 provides a mechanism whereby a network administrator may select or define a desired service level that is to be applied to a particular group of data flows within network 206.

(Emphasis added). Column 10, lines 33-49 of Cohen states:

> For example, embodiments are not required to always mark with a specified second DSCP value in response to detecting a flow that is marked using a specified first DSCP value. Multiple different marking values may be applied to packets at any point in the return path of the packet in response to detecting a particular marking value in the packet in an originating flow.
>
> Any of the foregoing embodiments also may be implemented on end device routers or other end station hosts.
>
> The DS field is defined also for version 6 of the Internet Protocol (IPv6). The foregoing embodiments may be used with IPv6 by

> storing reflective DSCP rules for IPv6 on edge devices or end nodes.
>
> In addition, embodiments are not limited to the context of packet data transmission using IP networks such as the Internet.

(Emphasis added). As such, Cohen appears to disclose that colors correspond to a particular service level associated with a QoS, that a forwarding policy may be based on the color of the packet, and that an administrator may define a service level applied to a data flow. Cohen further discloses that different marking values may be applied to packets based on "a particular marking value in the packet in an originating flow." However, Cohen does not in any way discuss a "services manager" not being able to obtain a DSCP value or what functions are performed if a "services manager" is unable to obtain a DSCP value.. The different marking values of Cohen are applied based on a marking value of a packet in an initial flow, not because a "services manager" was unable to obtain a DSCP value. Accordingly, Cohen fails to teach, suggest, or disclose "wherein if the services manager cannot obtain a DSCP value ... , the services manager determines an alternate traffic flow characterization for the traffic flow based on the traffic flow identification" as in Claim 4.

For at least the reasons discussed above, Applicants respectfully submit that Claims 4, 14, and 23 are in condition for allowance. As such, Applicants request reconsideration and withdrawal of the rejection of Claims 4, 14, and 23.

Applicants believe that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to

Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extension of time is needed for timely acceptance of papers submitted herewith, Applicants hereby petition for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extension fee to Deposit Account No. 19-0741.

Respectfully submitted,

Date May 7, 2009 By

FOLEY & LARDNER LLP
Customer Number: 23524
Telephone: (608) 258-4292
Facsimile: (608) 258-4258

Paul S. Hunter
Attorney for Applicants
Registration No. 44,787